



Universiteit Antwerpen
| Faculteit Rechten

GDPR en gezondheidsgegevens: overzicht van GBA-beslissingen

Prof. dr. Nils Broeckx

Studiedag *Patiëntendossier, beroepsgeheim, GDPR en EHDSR*

12 september 2025

Overzicht

1. **GDPR-boetes en zorginstellingen**
2. **Begrippen “verwerking van gezondheidsgegevens”**
3. **Verwerkingsverantwoordelijkheid in de zorg**
4. **Toegangsrechten m.b.t. EPD**
5. **Overige aspecten**

1. GDPR-boetes en zorginstellingen

Vooraf

- **Art. 56, lid 2 en 83 GDPR: correctieve maatregelen waaronder administratieve geldboetes**
 - € 2.000: verpleegorganisatie die recht op toegang schond (GBA nr. 13/2019, 17 december 2019)
 - € 20.000: medisch labo met o.a. onveilig patiëntenportaal (GBA nr. 127/2022, 19 augustus 2022)
 - € 200.000: ziekenhuis na (2^{de}) succesvolle ransomware-aanval (GBA nr. 166/2024, 17 december 2024)
- **Te onderscheiden van:**
 - Strafrechtelijke sancties (art. 222 e.v. Wet Bescherming Persoonsgegevens **maar ne bis in idem**)
 - Burgerrechtelijke sancties (cf. art. 82 GDPR en gemeen recht)
 - Tuchtrechtelijke sancties

Overheidsexceptie

- **Art. 5 Wet bescherming persoonsgegevens:**

Voor de toepassing van deze wet wordt verstaan onder "overheid" :

1° de Federale Staat, de deelstaten en lokale overheden;

2° de rechtspersonen van publiek recht die van de Federale Staat, de deelstaten of lokale overheden afhangen;

3° de personen, ongeacht hun vorm en aard, die :

- opgericht zijn met het specifieke doel te voorzien in behoeften van algemeen belang die niet van industriële of commerciële aard zijn; en

- rechtspersoonlijkheid hebben; en

- waarvan hetzij de activiteiten in hoofdzaak door de overheden of instellingen vermeld in de bepalingen onder 1° of 2°, worden gefinancierd, hetzij het beheer onderworpen is aan toezicht door deze overheden of instellingen, hetzij de leden van het bestuursorgaan, leidinggevend orgaan of toezichthoudend orgaan voor meer dan de helft door deze overheden of instellingen zijn aangewezen;

4° de verenigingen bestaande uit één of meer overheden als bedoeld in de bepalingen onder 1°, 2° of 3°.

- **Art. 221, §2 Wet Bescherming persoonsgegevens:**

§ 2. Het artikel 83 van de Verordening is niet van toepassing op de overheid en hun aangestelden of gemachtigden, tenzij het gaat om een publiekrechtelijke rechtspersoon die goederen of diensten aanbiedt op een markt.

Ratio legis: continuïteit vrijwaren

GBA nr. 166/2024, 17 december 2024

- € 200.000 geldboete voor **privaat** ziekenhuis na ransomware aanval
- **Strikt overheidsbegrip (art. 5 WBP):**
 - ZH niet exclusief in algemeen belang opgericht (want economische overwegingen)
 - Terugbetaling prestaties is niet overheidsfinanciering (BFM wel?)
 - Bevoegdheid AVIQ is geen 'beheer' want in casu geen rechtstreekse controle
- **Quid publiekrechtelijke zorginstellingen?**
 - Bieden goederen en diensten op een markt aan (art. 221, §2 WBP; cf. MvT)

2. Begrippen “verwerking van gezondheidsgegevens”

Vooraf

Art. 4 GDPR

(1) **“persoonsgegevens”**: **alle** informatie over een **geïdentificeerde of identificeerbare** natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

(2) **“verwerking”**: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, **zoals** het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

(...)

(15) **“gegevens over gezondheid”**: **persoonsgegevens** die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven [cf. art. 9 GDPR: strikter regime]

Art. 2, lid 1 GDPR

Deze verordening is van toepassing op de geheel of gedeeltelijk **geautomatiseerde** verwerking, alsmede op de verwerking van persoonsgegevens die in een **bestand** zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Ruime invulling

Inclusief

- ziektebriefje bedoeld voor de werkgever (GBA nr. 148/2023, 9 november 2023)
- informatie over alcohol- of drugsmisbruik i.k.v. enquête betreffende gezondheidsbeleid op school (GBA nr. 70/2025, 18 april 2025)
- lichaamstemperatuur bij koortsmeting (GBA nr. 75/2025, 24 april 2025; zie ook voorheen + GBA nr. 47/2022, 4 april 2022 & GBA nr. 48/2022, 4 april 2022)
- informatie over contact van WZC-bezoekers met besmette personen (GBA nr. 75/2025, 24 april 2025)
- loutere feit dat men sollicitant in een ziekenhuis is, waar enkel gevaccineerde sollicitanten worden aangenomen; vaccinatiestatus houdt verband met mogelijke evolutie van de gezondheidsstatus (GBA nr. 143/2021, 22 december 2021)

Maar niet onbegrensd

- Loutere feit dat een vrouw **“aanstaande moeder” is of reeds bevallen is** (in het kader van het aanbieden van babyspullen i.s.m. materniteiten) blijkt op zich geen gezondheidsgegeven (**schijnbaar GBA nr. 04/2021, 27 januari 2021**)
- **Verslag van medische raadpleging in ZSG**: hoewel verslag ongetwijfeld gezondheidsgegevens bevat, zijn sommige gegevens (bv. een beschrijving van de feiten van geweldpleging) mogelijk geen gezondheidsgegevens (**GBA nr. 103/2023, 26 juli 2023: wel zeer voorzichtig behandelen**)
- Registratie van lichaamstemperatuur bij koortsmeting is wél een gezondheidsgegeven, maar niet loutere feit dat de **temperatuur werd gecontroleerd** (**GBA nr. 75/2025, 24 april 2025**)

CAVEAT

Gezondheidsgegevens zonder verwerking?

- **Louter aflezen van lichaamstemperatuur** op thermometer, zonder registratie van temperatuur/koorts, is geen verwerking onder GDPR (GBA nr. 47/2022, 4 april 2022)
- **Louter mondelinge vermelding van arbeidsongeschiktheid** van een werknemer, voor zover geen vermelding in vergadernotulen, is geen verwerking onder GDPR (GBA nr. 115/2022, 19 juli 2022)

KRITIEK

3. Verwerkings- verantwoordelijkheid in de zorg

Vooraf

Art. 4 GDPR

(7) **"verwerkingsverantwoordelijke"**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, **alleen of samen** met anderen, **het doel van en de middelen** voor de verwerking van persoonsgegevens **vaststelt**; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen; [cf. EDPB Richtlijnen 07/2020]

(8) **"verwerker"**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat **ten behoeve van** de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

(...)

(10) **"derde"**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch **de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker** gemachtigd zijn om de persoonsgegevens te verwerken;

Belang:

- Art. 5, lid 2 GDPR: verwerkingsverantwoordelijke is (voornaamste) juridisch aanspreekpunt
- Art. 26 en 28 GDPR: contractueel luik

Feitelijke beoordeling geval per geval

- **Online afsprakenplatform A** (GBA nr. 149/2023, 10 november 2023; bevestigd MH 8 mei 2024)
 - Vermelding van professionele contactgegevens van gezondheidszorgbeoefenaars op website zonder dat beoefenaars daar per se van op de hoogte zijn of er controle over hebben
 - Beheerder van platform (commercieel bedrijf) is verwerkingsverantwoordelijke
 - Investeerder is geen verwerkingsverantwoordelijke want louter financiële bijdrage [quid louter wetenschappelijke input bij klinische studie?]

versus

- **Online afsprakenplatform B** (GBA nr. 62/2024, 25 april 2024; GBA nr. 62/2024 van 25 april 2024)
 - SaaS-contract voor online agendasysteem
 - Gezondheidszorgbeoefenaar is verwerkingsverantwoordelijke want beslist om het platform in te schakelen en bepaalt welke platformfunctionaliteiten hij gebruikt voor zijn zorgpraktijk
 - Aanbieder van agendasysteem is verwerker, ook al zijn er niet-onderhandelbare algemene voorwaarden en een aantal vooraf bepaalde functionaliteiten

Wat met individuele beoefenaars in zorginstelling?

- **Principe: rechtspersoon van de organisatie is verwerkingsverantwoordelijke**
 - Typisch ziekenhuisbeheerder:
 - Ziekenhuis i.v.m. audit-verslag van externe expert (GBA nr. 41/2020, 29 juli 2020)
 - Ziekenhuis i.v.m. kennisname abortus via 'afdelingsoverzicht' (GBA nr. 77/2022, 11 mei 2022)
 - Andere gevallen:
 - Medisch labo i.v.m. staalanalyse (GBA nr. 127/2022, 19 augustus 2022)
 - Externe preventiedienst i.v.m. psychosociaal verslag (GBA nr. 09/2023, 18 januari 2024)
- **Caveat**
 - Procedurele redenen waarom individuele beoefenaars niet gevisieerd worden?
 - In theorie gezamenlijke verwerkingsverantwoordelijkheid niet uitgesloten t.a.v. 'zelfstandige' personeelsleden [~ interpretatie van "rechtstreeks gezag"]
 - GBA nr. 64/2025, 1 april 2025: hiërarchisch leidinggevende binnen ziekenhuis treedt op als enige verwerkingsverantwoordelijke bij inzage in medisch dossier van (ex-)collega (*in casu* buiten de werkuren) zonder dat dit op enige wijze nodig was i.k.v. takenpakket

4. Toegangsrechten m.b.t. EPD

Vooraf

- **GDPR:** algemeen basiskader (o.a. rechtmatigheid, doelbinding, dataminimalisatie, *data protection by default*, passende technische en organisatorische maatregelen)
- **Kwaliteitswet:** toegang tot gezondheidsgegevens bij andere gezondheidszorgbeoefenaars (o.a. toestemming en therapeutische relatie)
- **Wet eHealth-platform:** technisch-organisatorische uitwerking via metahub-hub-systeem (opt-out + opt-in en therapeutische relatie)
- [EHDSR: toegangsdiensten voor primair gebruik]

GBA nr. 103/2023, 26 juli 2023

▪ Feiten

- klacht van patiënte (slachtoffer van seksueel geweld) tegen psycholoog van ziekenhuis
- psycholoog had toegang tot allerlei medische gegevens vanuit ZSG van ziekenhuis
- patiënte vreest dat informatie beschikbaar is voor al het zorgpersoneel

▪ Waarschuwing wegens mogelijke schending (i.k.v. artikelen 24 en 32 GDPR)

*“(…) que la défenderesse [het ziekenhuis] était et demeure tenue de mettre en oeuvre toutes les mesures techniques et organisationnelles de nature à garantir que les prestataires de soins et autres professionnels qui recourent à son système d’échange d’information **n’accèdent qu’aux seules données du dossier de patient nécessaires à leurs prestations respectives** et ce, dans le respect de l’ensemble du cadre juridique applicable dont, mais non exclusivement, le RGPD”*

Toegang op basis van *need-to-know*

Ziekenhuissoftware moet instellen van toegangsrechten op basis van verschillende criteria toelaten (identiteit, hoedanigheid, categorieën persoonsgegevens, gebruiksdoel, duurtijd en confidentialiteitsgraad)

GBA nr. 64/2025, 1 april 2025

▪ Feiten

- Werkneemster van ziekenhuis wordt ontslagen door directie, mede i.v.m. gezondheidstoestand
- Hiërarchisch leidinggevende kijkt de dag voor het ontslaggesprek het medisch dossier van werkneemster in buiten werkuren en zonder dat dit nodig was voor haar taken

▪ Geen inbreuk door ziekenhuis (opnieuw i.k.v. artikelen 24 en 32 GDPR)

(...) que ces mesures techniques et organisationnelles ne peuvent pas non plus conduire à la mise en péril de la continuité des soins des patients, ce qui pourrait placer la santé de ces derniers en danger (...) il n'est *pas toujours possible de déterminer à l'avance* quels membres du personnel médical ou paramédical d'un hôpital – lequel personnel est pluridisciplinaire – seront amenés à entrer en contact avec un patient, *ce qui justifie que l'ensemble du personnel médical et paramédical dispose d'un accès aux dossiers médicaux des patients de l'hôpital.*"

Geen afwijking maar wel 'aanvulling' op GBA nr. 103/2023

Ruimte voor flexibiliteit in toegangsrechtenbeheer in het licht van continuïteit en multidisciplinaire zorgaanpak volgens regels van de kunst

Verschillende modellen van toegangsmatrix denkbaar

Cf. overweging 19 EHDSR

“Tijdige en volledige toegang van gezondheidswerkers tot de medische dossiers van patiënten is van fundamenteel belang om de continuïteit van de zorg te waarborgen, dubbel werk en fouten te voorkomen en de kosten te drukken. (...) Aangezien het moeilijk is om vooraf uitputtend vast te stellen welke gegevens van de bestaande gegevens in prioritaire categorieën vanuit medisch oogpunt relevant zijn in een specifieke zorgperiode, moeten gezondheidswerkers ruime gegevenstoegang hebben. Wanneer gezondheidswerkers gegevens van hun patiënten inzien, moeten zij het toepasselijk recht en toepasselijke gedragscodes, deontologische richtsnoeren en andere bepalingen inzake ethisch gedrag met betrekking tot het delen van of de toegang tot informatie naleven, met name in levensbedreigende of extreme situaties. Overeenkomstig Verordening (EU) 2016/679 moeten zorgaanbieders, opdat hun toegang beperkt blijft tot wat relevant is voor een specifieke zorgperiode, bij het gebruik van persoonlijke elektronische gezondheidsgegevens het beginsel van minimale gegevensverwerking in acht nemen en zich alleen toegang verschaffen tot gegevens waarvan het gebruik strikt noodzakelijk en gerechtvaardigd is voor een bepaalde dienst.”

5. Overige aspecten

Veilige verwerking (art. 5, lid 1, f GDPR)

- **Algemeen:**

- Vereiste van “passende” veiligheidsmaatregelen
- “Minimale Normen” (Kruispuntbank van de Sociale Zekerheid) alsook “Referentiemaatregelen voor beveiliging van persoonsgegevens” (GBA) zijn nuttige referentie voor een ziekenhuis (GBA nr. 166/2024, 17 december 2024)

- **Specifiek (GBA nr. 166/2024, 17 december 2024)**

- Wachtwoorden: min. 12 karakters en 2FA
- Loggings: wie, wanneer, hoe en wat? + loggings gedurende redelijke termijn apart bewaren [personeel informeren]
- Structurele en wederkerende training: aanwezigheid van bepaalde personeelsleden op studiedag over cyberbeveiliging volstaat niet

Transparantie (art. 5, lid 1, a GDPR)

■ Regime art. 13 vs. art. 14 GDPR

- Er is ook sprake van een *rechtstreekse* inzameling (art. 13 GDPR) wanneer de gegevens verkregen worden door rechtstreekse monitoring of observatie van de patiënt via wearables, camera's of andere informatietechnologie (cf. GBA nr. 47/2022, 4 april 2022, + GBA nr. 48/2022, 4 april 2022 i.v.m. temperatuursmeting via warmtebeeldcamera's)

■ Wijze van informatieverstrekking

- Het volstaat niet om een privacyreglement aan te plakken in de lokalen van een medisch labo; de informatie moet ook op de website staan, nu deze website gebruikt werd voor communicatie met patiënt, m.n. online inzage in testresultaten (GBA nr. 127/2022, 19 augustus 2022)

Opslagbeperking (art. 5, lid 1, e GDPR)

- **Schending:** persoonsgegevens van moeders en pasgeborenen gedurende 18 jaar bewaren met het oog op het aanbieden van babyspullen (GBA nr. 04/2021, 27 januari 2021)
- **Geen schending:** bewaring van persoonsgegevens van radioloog i.k.v. audit gedurende verjaringstermijn (cf. GBA nr. 41/2020, 29 juli 2020)
[maar evalueren of alle persoonsgegevens wel even lang bewaard moeten blijven]

Q&A

Nils.broeckx@uantwerpen.be